# Topic 5: The Internet and Its Uses

Keyword sheet - Cambridge IGCSE Computer Science 0984. Tick each term once you can define it from memory.

| Keyword | Definition | Know it? |
|---|---|---|
| **Internet** | A worldwide network of interconnected networks, the infrastructure that carries services such as the web and email. | |
| **World Wide Web (WWW)** | A collection of web pages and resources accessed over the internet using HTTP/HTTPS and a browser. | |
| **URL** | Uniform resource locator: the address of a web resource, made of protocol, domain name and path. | |
| **HTTP / HTTPS** | Protocols for transferring web pages; HTTPS adds encryption using TLS. | |
| **Web browser** | Application that requests web pages, renders HTML and displays them to the user. | |
| **Web server** | Computer that stores web pages and sends them in response to requests. | |
| **DNS** | Domain name system: translates domain names into IP addresses. | |
| **IP address** | Unique address identifying a device on a network. | |
| **Cookie** | Small text file stored by a browser that holds information about the user. | |
| **Session / persistent cookie** | Session cookies are deleted when the browser closes; persistent cookies remain until they expire or are deleted. | |
| **Digital currency** | Money that exists only electronically and is not physical cash. | |
| **Cryptocurrency** | Digital currency secured by cryptography and usually decentralised, e.g. Bitcoin. | |
| **Blockchain** | A decentralised, linked list of blocks of transactions secured by hashing, making records very difficult to alter. | |
| **Malware** | Malicious software designed to damage, disrupt or gain unauthorised access to a system. | |
| **Virus** | Malware that attaches to a program or file and replicates when it is run. | |
| **Worm** | Self-replicating malware that spreads across networks without user action. | |
| **Trojan horse** | Malware disguised as legitimate software. | |
| **Spyware** | Malware that secretly records user activity, e.g. keylogging. | |
| **Ransomware** | Malware that encrypts or locks data and demands payment for its release. | |
| **Phishing** | Fraudulent messages designed to trick users into revealing personal data or credentials. | |
| **Pharming** | Malicious code redirects users to a fake website even when the correct address is entered. | |
| **Hacking** | Gaining unauthorised access to a computer system. | |

| Keyword | Definition | Know it? |
|---|---|---|
| **DDoS attack** | Distributed denial of service: many computers flood a server with requests so that legitimate users cannot access it. | |
| **Brute-force attack** | Systematically trying all possible passwords or keys until the correct one is found. | |
| **Firewall** | Hardware or software that monitors network traffic and blocks traffic according to rules. | |
| **Authentication** | Verifying identity using something you know, have or are: passwords, tokens, biometrics, two-factor. | |
| **Biometrics** | Authentication using unique biological features such as fingerprints or facial recognition. | |
| **Proxy server** | Intermediary between a user and the internet that can filter requests, cache pages and hide user addresses. | |
| **Antivirus / anti-malware** | Software that scans for, detects and removes malicious code. | |